Руководителю проекта

«Разработка комплекта документации по правовому обеспечению функционирования системы DLP»

Агеевой Елене Александровне

от Участника проекта

«Разработка комплекта документации по правовому обеспечению функционирования системы DLP»

Великанов Иван Вадимович

Аналитическая записка

Законность использования системы DLP в соответствии с Регламентом GDPR

В результате расширения сферы услуг компании на территорию Европы, следует подготовить перечень правил под Регламент законодательства ЕС, а именно регламент - GDPR — (General Data Protection Regulation). GDPR имеет экстерриториальное действие и применяется ко всем компаниям, обрабатывающим персональные данные резидентов и граждан ЕС, независимо от местонахождения такой компании. Соответственно компания должна соответствовать правилам регламента.

Для соответствия требованиям GDPR необходимо разработать внутренние политики защиты данных, обучать персонал, проводить проверки деятельности по обработке данных, вести документацию по процессам обработки, внедрять меры по встроенной системе

конфиденциальности, а также назначить сотрудника ответственного за обработку персональных данных.

В случае использования компанией DLP-системы или других средств мониторинга активности пользователей, также необходимо соблюдать основные правила для соответствия процессу мониторинга требованиям Регламента GDPR:

- Любая переписка сотрудников, в том числе с использованием сервиса корпоративной электронной почты, должна считаться строго конфиденциальной;
- Организация может принять правила и внедрить средства автоматизированной блокировки (без предоставления возможности чтения сообщений), но для этого необходимо произвести оценку баланса интересов (работника и работодателя) и уведомить работников. При этом следует четко обозначить цель такого контроля и обосновать необходимость. В качестве обоснования необходимости может использоваться статья GDPR, регламентирующая необходимость защиты от утечек персональных данных;
- В ряде случаев (например, при болезни сотрудника и оправданной рабочей необходимости) допускается поиск сообщений по теме/отправителю/получателю и/или просмотр отдельных сообщений почты. Открытие (просмотр) почтовых сообщений допускается только в присутствии свидетелей. По факту поиска и/или открытия сообщений создается отчет с указанием причины, цели, участников и перечня лиц, которые были уведомлены о содержании переписки. Этот отчет должен быть подписан участниками и направлен сотруднику без задержки. После прекращения трудовых отношений сотрудник может потребовать

закрытия своего почтового ящика, а дальнейшее его использование возможно только по соглашению с сотрудником;

- Использование DLP-систем, в которых не реализован принцип «четырех глаз» (four eyes principle)[1] для разграничения доступа к событиям и инцидентам, считается нелегитимным.

Перед началом внедрения DLP-системы, необходимо провести DPIA «Data protection impact assessment», что подразумевает оценку соразмерности. Оценка соразмерности проводится для понимания того, может ли компания обойтись без применения средств мониторинга активности работников, если это возможно. Например, если риск утечки ПДн через корпоративную почту будет минимален, то применять средства перехватал корпоративной почты сотрудников не рекомендуется.

Сотрудники должны получать полную информацию о мониторинге и быть в полной мере уведомлены о происходящем мониторинге (какими средствами он осуществляется, какие каналы передачи используются, какие данные могут быть перехвачены и т.д.).

Правовым основанием для мониторинга данных стоит использовать «легитимный интерес» (т.е. интерес в защите персональных данных). В то же время не стоит полагаться только на согласие, данное работником для проведения мониторинга, т.к. согласие может быть отозвано работников в любой момент, и он этом может быть не оповещен работник ИБ, администрирующий системы. Таким образом, не приостановленный в нужный момент мониторинг за работником может быть расценен как нарушение.

[1] Под этим понимается организация двойного независимого параллельного контроля